

CYBER INVESTIGATIONS

6 Month Course
25 February 2025



CYBER SECURITY INSTITUTE
Solutions • Advisory • Learning



This practical, hands-on course focuses on establishing a foundation in Cyber Security by introducing candidates to cyber-crime, attack methods, and managing cyber risks.

Developed by the Cyber Security Institute (CSI) and offered in collaboration with the Cape Peninsula University of Technology (CPUT) and the French South African Institute of Technology (FSATI). This course is suitable for investigators and investigation teams within the corporate environment and public sectors who are required to track online trails or utilise tools to solve online crimes. It is also intended for professionals and investigative journalists involved in investigations such as fraud, espionage, data theft, and cyber vetting.

Mode Of Learning

February 2025 – July 2025

Learning will be conducted through a facilitated online format, utilising an e-learning platform to provide an interactive and engaging educational experience. Additionally, hands-on practical sessions and virtual labs will be conducted offering participants the opportunity to apply theoretical knowledge in a real-world context. This blend of online facilitated learning and scheduled virtual sessions aims to create a comprehensive and dynamic learning environment, ensuring a well-rounded educational experience for participants.

Duration

This course is designed for individuals embarking on a career in Cyber Security or performing security functions.





Important Course Information

Requirements

Applicants should have a Matric certificate or equivalent qualification with suitable IT knowledge, Internet access, and a PC or laptop on which applications can be installed and services accessed.

Intake

We have two main intakes, one at the end of February and another at the end of June. Additional intakes may be scheduled depending on application volumes and requirements.

Costs & Duration

6-months and R10,500 all-inclusive course



Course Overview

- Reconnaissance
- Online services and tools
- Metadata Encryption & Decryption
- Digital signatures
- Online investigations
- Crime Scene Management
- Documenting evidence
- Investigation Process
- Chain of Evidence
- Protocols and emails
- URLs & DNS information
- Timelines
- Decryption and deciphering
- Virtual Currencies
- Cyber criminology
- Introduction to the attack process
- Introduction to attack vectors
- Social networks (i.e., attacks via Facebook, Twitter, etc.)
- Dark and hidden web
- Threat actors
- Data Collection
- Social Media
- OSINT
- HUMINT
- SOCMINT